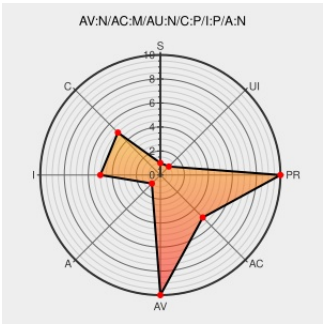
CVE-2011-4354

Published on: 01/26/2012 12:00:00 AM UTC

Last Modified on: 02/13/2023 12:13:16 AM UTC

CVE-2011-4354

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Openssl from Openssl contain the following vulnerability:

crypto/bn/bn_nist.c in OpenSSL before 0.9.8h on 32-bit platforms, as used in stunnel and other products, in certain circumstances involving ECDH or ECDHE cipher suites, uses an incorrect modular reduction algorithm in its implementation of the P-256 and P-384 NIST elliptic curves, which allows remote attackers to obtain the private key of a TLS server via multiple handshake attempts.

CVE-2011-4354 has been assigned by secalert@redhat.com to track the vulnerability

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
oss-security - CVE-2011-4354 OpenSSL 0.9.8g (32-bit builds) bug leaks ECC private keys	openwall.com text/html	MLIST [oss-security] 20111201 CVE-2011-4354 OpenSSL 0.9.8g (32-bit builds) bug leaks ECC private keys
#1593: BN_nist_mod_384 gives wrong answers	web.archive.org text/html Inactive Link Not Archived	CONFIRM rt.openssl.org/Ticket/Display.html?id=1593&user=guest&pass=guest
'[openssl.org #1593] BN_nist_mod_384 gives wrong answers' thread - MARC	marc.info text/html	CONFIRM marc.info/?t=119271238800004
757909 – (CVE-2011-4354) CVE-2011-4354 openssl: ECC private leak (disclosure of TLS server's private key)	bugzilla.redhat.com text/html	CONFIRM bugzilla.redhat.com/show_bug.cgi?id=757909

No Description Provided	cvs.openssl.org Inactive Link Not Archived	CONFIRM cvs.openssl.org/filediff?f=openssl/crypto/bn/bn_nist.c&v1=1.14&v2=1.21
Debian -- Security Information -- DSA-2390-1 openssl	www.debian.org Depreciated Link text/html	DEBIAN DSA-2390
	crypto.di.uminho.pt application/zip	MISC crypto.di.uminho.pt/CACE/CT-RSA2012-openssl-src.zip
Cryptology ePrint Archive: Report 2011/633	eprint.iacr.org text/html	MISC eprint.iacr.org/2011/633

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openssl	Openssl	0.9.1c	All	All	All
Application	Openssl	Openssl	0.9.2b	All	All	All
Application	Openssl	Openssl	0.9.3	All	All	All
Application	Openssl	Openssl	0.9.3a	All	All	All
Application	Openssl	Openssl	0.9.4	All	All	All
Application	Openssl	Openssl	0.9.5	All	All	All
Application	Openssl	Openssl	0.9.5	beta1	All	All
Application	Openssl	Openssl	0.9.5	beta2	All	All
Application	Openssl	Openssl	0.9.5a	All	All	All
Application	Openssl	Openssl	0.9.5a	beta1	All	All
Application	Openssl	Openssl	0.9.5a	beta2	All	All
Application	Openssl	Openssl	0.9.6	All	All	All
Application	Openssl	Openssl	0.9.6	beta1	All	All
Application	Openssl	Openssl	0.9.6	beta2	All	All
Application	Openssl	Openssl	0.9.6	beta3	All	All
Application	Openssl	Openssl	0.9.6a	All	All	All
Application	Openssl	Openssl	0.9.6a	beta1	All	All
Application	Openssl	Openssl	0.9.6a	beta2	All	All
Application	Openssl	Openssl	0.9.6a	beta3	All	All
Application	Openssl	Openssl	0.9.6b	All	All	All

Application	Openssl	Openssl	0.9.6c	All	All	All
Application	Openssl	Openssl	0.9.6d	All	All	All
Application	Openssl	Openssl	0.9.6e	All	All	All
Application	Openssl	Openssl	0.9.6f	All	All	All
Application	Openssl	Openssl	0.9.6g	All	All	All
Application	Openssl	Openssl	0.9.6h	All	All	All
Application	Openssl	Openssl	0.9.6i	All	All	All
Application	Openssl	Openssl	0.9.6j	All	All	All
Application	Openssl	Openssl	0.9.6k	All	All	All
Application	Openssl	Openssl	0.9.6l	All	All	All
Application	Openssl	Openssl	0.9.6m	All	All	All
Application	Openssl	Openssl	0.9.7	All	All	All
Application	Openssl	Openssl	0.9.7	beta1	All	All
Application	Openssl	Openssl	0.9.7	beta2	All	All
Application	Openssl	Openssl	0.9.7	beta3	All	All
Application	Openssl	Openssl	0.9.7	beta4	All	All
Application	Openssl	Openssl	0.9.7	beta5	All	All
Application	Openssl	Openssl	0.9.7	beta6	All	All
Application	Openssl	Openssl	0.9.7a	All	All	All
Application	Openssl	Openssl	0.9.7b	All	All	All
Application	Openssl	Openssl	0.9.7c	All	All	All
Application	Openssl	Openssl	0.9.7d	All	All	All
Application	Openssl	Openssl	0.9.7e	All	All	All
Application	Openssl	Openssl	0.9.7f	All	All	All
Application	Openssl	Openssl	0.9.7g	All	All	All
Application	Openssl	Openssl	0.9.7h	All	All	All
Application	Openssl	Openssl	0.9.7i	All	All	All
Application	Openssl	Openssl	0.9.7j	All	All	All
Application	Openssl	Openssl	0.9.7k	All	All	All
Application	Openssl	Openssl	0.9.7l	All	All	All
Application	Openssl	Openssl	0.9.7m	All	All	All
Application	Openssl	Openssl	0.9.8	All	All	All
Application	Openssl	Openssl	0.9.8a	All	All	All
Application	Openssl	Openssl	0.9.8b	All	All	All
Application	Openssl	Openssl	0.9.8c	All	All	All
Application	Openssl	Openssl	0.9.8d	All	All	All

Application	Openssl	Openssl	0.9.8e	All	All	All
Application	Openssl	Openssl	0.9.8f	All	All	All
Application	Openssl	Openssl	All	All	All	All
Application	Openssl	Openssl	0.9.1c	All	All	All
Application	Openssl	Openssl	0.9.2b	All	All	All
Application	Openssl	Openssl	0.9.3	All	All	All
Application	Openssl	Openssl	0.9.3a	All	All	All
Application	Openssl	Openssl	0.9.4	All	All	All
Application	Openssl	Openssl	0.9.5	All	All	All
Application	Openssl	Openssl	0.9.5	beta1	All	All
Application	Openssl	Openssl	0.9.5	beta2	All	All
Application	Openssl	Openssl	0.9.5a	All	All	All
Application	Openssl	Openssl	0.9.5a	beta1	All	All
Application	Openssl	Openssl	0.9.5a	beta2	All	All
Application	Openssl	Openssl	0.9.6	All	All	All
Application	Openssl	Openssl	0.9.6	beta1	All	All
Application	Openssl	Openssl	0.9.6	beta2	All	All
Application	Openssl	Openssl	0.9.6	beta3	All	All
Application	Openssl	Openssl	0.9.6a	All	All	All
Application	Openssl	Openssl	0.9.6a	beta1	All	All
Application	Openssl	Openssl	0.9.6a	beta2	All	All
Application	Openssl	Openssl	0.9.6a	beta3	All	All
Application	Openssl	Openssl	0.9.6b	All	All	All
Application	Openssl	Openssl	0.9.6c	All	All	All
Application	Openssl	Openssl	0.9.6d	All	All	All
Application	Openssl	Openssl	0.9.6e	All	All	All
Application	Openssl	Openssl	0.9.6f	All	All	All
Application	Openssl	Openssl	0.9.6g	All	All	All
Application	Openssl	Openssl	0.9.6h	All	All	All
Application	Openssl	Openssl	0.9.6i	All	All	All
Application	Openssl	Openssl	0.9.6j	All	All	All
Application	Openssl	Openssl	0.9.6k	All	All	All
Application	Openssl	Openssl	0.9.6l	All	All	All
Application	Openssl	Openssl	0.9.6m	All	All	All
Application	Openssl	Openssl	0.9.7	All	All	All

Application	Openssl	Openssl	0.9.7	beta1	All	All
Application	Openssl	Openssl	0.9.7	beta2	All	All
Application	Openssl	Openssl	0.9.7	beta3	All	All
Application	Openssl	Openssl	0.9.7	beta4	All	All
Application	Openssl	Openssl	0.9.7	beta5	All	All
Application	Openssl	Openssl	0.9.7	beta6	All	All
Application	Openssl	Openssl	0.9.7a	All	All	All
Application	Openssl	Openssl	0.9.7b	All	All	All
Application	Openssl	Openssl	0.9.7c	All	All	All
Application	Openssl	Openssl	0.9.7d	All	All	All
Application	Openssl	Openssl	0.9.7e	All	All	All
Application	Openssl	Openssl	0.9.7f	All	All	All
Application	Openssl	Openssl	0.9.7g	All	All	All
Application	Openssl	Openssl	0.9.7h	All	All	All
Application	Openssl	Openssl	0.9.7i	All	All	All
Application	Openssl	Openssl	0.9.7j	All	All	All
Application	Openssl	Openssl	0.9.7k	All	All	All
Application	Openssl	Openssl	0.9.7l	All	All	All
Application	Openssl	Openssl	0.9.7m	All	All	All
Application	Openssl	Openssl	0.9.8	All	All	All
Application	Openssl	Openssl	0.9.8a	All	All	All
Application	Openssl	Openssl	0.9.8b	All	All	All
Application	Openssl	Openssl	0.9.8c	All	All	All
Application	Openssl	Openssl	0.9.8d	All	All	All
Application	Openssl	Openssl	0.9.8e	All	All	All
Application	Openssl	Openssl	0.9.8f	All	All	All

cpe:2.3:a:openssl:openssl:0.9.1c:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.2b:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.3:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.3a:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.4:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.5:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.5:beta1:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.5:beta2:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.5a:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.5a:beta1:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.5a:beta2:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6:beta1:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6:beta2:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6:beta3:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6a:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6a:beta1:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6a:beta2:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6a:beta3:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6b:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6c:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6d:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6e:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6f:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6g:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6h:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6i:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6j:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6k:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6l:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6m:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7:beta1:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7:beta2:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7:beta3:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7:beta4:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7:beta5:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7:beta6:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7a:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7b:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7c:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7d:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7e:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7f:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7g:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7h:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7i:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7j:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7k:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7l:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7m:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.8:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.8a:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.8b:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.8c:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.8d:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.8e:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.8f:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:*:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.1c:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.2b:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.3:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.3a:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.4:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.5:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.5:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.5:beta1:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.5:beta2:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.5a:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.5a:beta1:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.5a:beta2:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6:beta1:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6:beta2:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6:beta3:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6a:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6a:beta1:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6a:beta2:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6a:beta3:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6b:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6c:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6d:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6e:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6f:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6g:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6h:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6i:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6j:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6k:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6l:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.6m:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7:beta1:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7:beta2:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7:beta3:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7:beta4:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7:beta5:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7:beta6:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7a:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7b:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7c:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7d:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7e:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7f:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7g:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7h:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7i:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7j:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7k:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7l:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.7m:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.8:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.8a:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.8b:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.8c:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.8d:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.8e:*:*:*:*:*:x86:*:

cpe:2.3:a:openssl:openssl:0.9.8f:*:*:*:*:*:x86:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→

CVE.report and Source URL Uptime Status status.cve.report